2019

ALI Data Privacy: Overview and Black Letter Text

Daniel J. Solove
George Washington University Law School, dsolove@law.gwu.edu

Paul M. Schwartz

ALI Data Privacy: Overview and Black Letter Text

BY
DANIEL J. SOLOVE*
&
PAUL M. SCHWARTZ**

ABSTRACT

In this Essay, the Reporters for the American Law Institute Principles of Law, Data Privacy provide an overview of the project as well as the text of its black letter. The Principles aim to provide a blueprint for policymakers to regulate privacy comprehensively and effectively.

The United States has long remained an outlier in privacy law. While numerous nations have enacted comprehensive privacy laws, the U.S. has clung stubbornly to a fragmented, inconsistent patchwork of laws. Moreover, there long has been a vast divide between the approaches of the U.S. and European Union (EU) to regulating privacy – a divide that many consider to be unbridgeable.

The Principles propose comprehensive privacy principles for legislation that are consistent with certain key foundations in the U.S. approach to privacy, yet that also align the U.S. with the EU. Additionally, the Principles attempt to breathe new life into the moribund and oft-criticized U.S. notice-and-choice approach, which has remained firmly rooted in U.S. law. Drawing from a vast array of privacy laws and frameworks, and with a balance of innovation, practicality, and compromise, the Principles aim to guide policymakers in advancing U.S. privacy law.

---

* John Marshall Harlan Research Professor of Law, George Washington University Law School. The views in this essay about the *ALI Principles of Law, Data Privacy* are those of Paul Schwartz and Daniel Solove only. The authoritative text about the meaning of the Principles is the main document itself, which contains comments, notes, and illustrations.
** Jefferson E. Peyser Professor at UC Berkeley School of Law, and Director, Berkeley Center for Law and Technology.

INTRODUCTION

Data privacy law in the United States is currently a bewildering assortment of many types of federal and state law that differ significantly from each other.[1] While many countries follow the approach of the European Union (EU) by enacting a comprehensive privacy law,[2] the approach of the U.S. remains highly fragmented, inconsistent, and gap-ridden. Calls for a new direction in U.S. privacy law are becoming more frequent and are emerging from all directions.[3] The path forward, however, remains quite murky. Is there a meaningful and practical way for U.S. privacy law to advance? Can U.S. privacy law become more consistent with the law of the EU without making a radical break from its foundations?

These questions are ones with which scholars and policymakers have long struggled. It is because these questions are so difficult and because finding a resolution to them is so important that the American Law Institute decided to develop a project devoted to articulating 21st century concepts of privacy law, namely, the *Principles of Law, Data Privacy* (the "*Principles*"). It was our honor to serve as the Reporters for this project. The ALI's mission is "to promote the clarification and simplification of the law and its better adaptation to social needs, to secure the better administration of justice, and to encourage and carry on scholarly and scientific legal work."[4] The ALI has produced a remarkable number of projects that have exercised a profound influence on the law, including the Uniform Commercial Code, the Model Penal Code, and various Restatements of the Law, including the celebrated Restatement (Second) of Torts.

---

[1] For a concise introduction, see DANIEL SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 36-39 (6th edition 2018).

[2] Paul M. Schwartz, *Global Data Privacy: the EU Way*, 94 N.Y.U. Law Review – (forthcoming 2019).

[3] For example, in a speech in Brussels to EU data protection commissioners, Tim Cook, CEO of Apple, told EU officials, "It is time for the rest of the world—including my home country—to follow your lead." Tim Cook, CEO, Apple, Remarks Before the International Conference of Data Protection & Privacy Commissioners (Oct. 24, 2018).

[4] ALI, *How the Institute Works*, https://www.ali.org/about-ali/how-institute-works/.

Before these *Principles*, the ALI's only foray into privacy was the short section in the Restatement (Second) of Torts establishing the four privacy torts in 1977.[5] These four torts have not proven well-suited to contemporary privacy problems involving organizations collecting and using vast amounts of personal data.[6] With the *Principles*, the ALI has finally weighed in on privacy in the Twenty-First Century. The ALI categorizes this project as a "Principles" project. As explained by the ALI, "Principles are primarily addressed to legislatures, administrative agencies, or private actors. They can, however, be addressed to courts when an area is so new that there is little established law."[7] Accordingly, as a Principles project, the *Principles of Law, Data Privacy* seeks to provide guidance for the evolution of U.S. data privacy law toward a more comprehensive and coherent approach. The ALI approved these *Principles* in May 2019 following a seven-year process.[8]

Data privacy law, which is sometimes referred to as "information privacy law," concerns the collection, use, and disclosure of personal data.[9] The last few decades have witnessed a torrent of legislative, regulatory, and judicial activity regarding data privacy around the world. At present, 132 countries have privacy laws.[10] According to Graham Greenleaf, who tracks these developments, "Fifty countries have enacted new data privacy laws in the first nine years of this decade, an average of 5.5 per year."[11] Among the 231

---

[5] Restatement (Second) of Torts § 652 (1977).

[6] For criticisms of the privacy torts, see Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 Cal. L. Rev. 2007 (2010); Neil M. Richards & Daniel Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 Cal. L. Rev. 1887 (2010).

[7] ALI, *How the Institute Works*, https://www.ali.org/about-ali/how-institute-works/.

[8] The Principles were created not just by us, but also by our advisory group and many ALI members who contributed greatly to this project. The ALI process is a wonderful one — a thoughtful constructive discussion about how to craft meaningful regulation between practitioners, judges, and academics, among others.

[9] For a discussion of the different nomenclature used in this area of law, see Schwartz, *Global Data Privacy*, supra note 2, at --.

[10] Graham Greenleaf, *Global Data Privacy Laws 2019: New Eras for International Standards*, 157 Privacy Laws & Business International Report 14 (2019).

[11] Id. at 4.

countries surveyed by Greenleaf, about 57% now have data privacy laws.[12]

U.S. data privacy law remains an outlier among regulatory approaches around the world. The vast majority of countries have a comprehensive privacy law modeled after the law of the European Union (EU). The EU initially approached data privacy law with the Data Protection Directive of 1995.[13] The Directive set out standards for information privacy and mandated that each member nation adopt a comprehensive privacy law according to its requirements.[14] About 20 years later, in 2016, in an attempt to create greater harmonization among the law of EU member nations, and to update its law, the EU passed the General Data Protection Regulation (GDPR).[15] The GDPR became effective in May 2018. The Directive and the GDPR, its successor, have been the most influential approach to data privacy worldwide.[16] Most countries have enacted laws closer to the EU approach than to the U.S. approach. In the judgment of Greenleaf, "[S]omething reasonably described as 'European standard' data privacy laws are becoming the norm in most parts of the world with data privacy laws." [17]

The divergence between the privacy law of the U.S. and that of the EU has led to significant tensions and problems for smooth transborder data flows and efficient commerce between EU member nations and the U.S.[18] EU data privacy law has long required that before personal data about persons in the EU can be transferred to other countries,

---

[12] Id. at 4.

[13] European Parliament and Council Directive 95/46/EC – on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 [hereinafter Directive].

[14] Id.

[15] Regulation of the European Parliament and of the Council of 27 April 2016 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (May 4, 2016)[hereinafter GDPR].

[16] Schwartz, *Global Data Privacy Law*, supra note 2, at --.

[17] Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*, 2 Int'l Data Privacy L. 68, 77 (2011).

[18] For an early and important look at these issues, see PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 197-202 (1998).

those countries must have an "adequate level of protection."[19] The EU has not found the United States to have an adequate level of protection.[20] As a result, more cumbersome data transfer mechanisms must be used, such as the Standard Contractual Clauses, Binding Corporate Rules (BCRs), or the Privacy Shield Framework.[21]

U.S. privacy law is currently unwieldy and conflicting. The state of this area of U.S. law has led many foreign nations to discount the protections that do exist in the U.S. New laws continue to emerge in many states, which further contributes to the vast patchwork of inconsistent laws.[22] Because of these problems, advocates and industry have both started to push for a comprehensive federal data privacy law. But there remains significant skepticism that a meaningful compromise can be reached on a comprehensive federal law as well as strong doubts that U.S. privacy law can ever be brought into harmony with the GDPR.[23]

Although this skepticism appears widely shared, we contend that it is possible to craft a comprehensive approach to data privacy for the U.S. that bridges the divide with the EU. The true proof of our thesis is in the *Principles* themselves, which we publish as part of this Essay. As Reporters on the *Principles*, we faced choices about many challenging and contentious privacy issues. This Essay provides an overview of the approaches and solutions to these issues taken in the *Principles*, and it explains why we opted for these approaches over others. We then present the *Principles* themselves.

The *Principles* are not an attempt to write our ideal privacy law as if drafting on a blank slate. Nor is it an attempt to restate existing law.

---

[19] Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 Geo. L.J. 115 (2017).

[20] Indeed, in a non-binding opinion in 1999, the EU's Article 29 Working Party opined that the U.S. lacked adequate protection for personal data. Article 29 Working Party, *Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States* 2 (Jan. 26, 1999).

[21] For an overview, see SOLOVE & SCHWARTZ, supra note 1, at 1173-1203.

[22] See Matt Dumiak, *Introducing state privacy legislation amidst national privacy law discussions*, SC Magazine (May 21, 2019), at https://www.scmagazine.com/home/opinion/executive-insight/introducing-state-privacy-legislation-amidst-national-privacy-law-discussions/.

[23] John Hendel, *"Embarrassing": Congress stumbles in push for a consumer privacy law,* Politico (July 12, 2019), at https://www.politico.com/story/2019/07/12/congress-consumer-privacy-bill-1582540.

Instead, it is something in between. We build on foundations in existing law, seek fidelity to U.S. privacy law foundations, and attempt to advance the law progressively without clashing with core commitments or introducing concepts that are without precedent.

Overall, in the *Principles,* we aim to demonstrate how U.S. privacy law can maintain its essential commitments, build upon existing foundations, and end up in a place that is close to the GDPR, which is currently the most important global privacy benchmark. The *Principles* reflect our judgment about how far U.S. law can be pushed—at least within the ALI process, which requires approval first by a group of senior advisors, the Council, and then by the Members as a whole. It is an interesting question as to whether we could have pushed further in one direction or another. We welcome this discussion. Privacy law is constantly evolving, and today marks just a single stage in the evolution of this area of law. We hope that the *Principles* contribute to this evolution as other ALI projects have done in their respective fields.

We also have taken some new approaches to certain issues that have not yet been tried in quite the same fashion. Our primary contribution in this regard is to attempt to breathe new life into what has become known as the "notice-and-choice approach" that predominates much of U.S. privacy law.[24] Under this approach, organizations provide a statement about their privacy practices (notice), and individuals then can exercise some form of choice about their data (often to opt out of certain uses or transfers).[25] Numerous commentators have pointed out that the notice-and-choice approach has been ineffective, with many calling it an outright failure.[26] Most

---

[24] For a critical account of notice-and-choice, see Schwartz & Peifer, *Transatlantic Data Privacy Law*, supra note 19, at 136-137.

[25] Id.

[26] See, e.g., CHRISTOPHER HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 365 (2016)("The notice and consent regime is a rigged game, guaranteed to result in a company's getting the data they want with no guarantees against transgressive use of it."); Paul M. Schwartz, *Internet Privacy and the State*, 32 Conn. L. Rev. 815, 821-23 (2000)(noting multiple reasons for the failure of "self-reliant consent" for privacy on the Internet). Regarding the shortcomings of "information mandates" in a variety of settings, see OMRI BEN-SHAHAR & CARL SCHNEIDER, MORE THAN YOU WANT TO KNOW: THE FAILURE OF MANDATED CONSENT

people do not read privacy notices, do not understand them, are not provided with meaningful choices, and lack the understanding to make the choices right for them.[27] The *Principles* attempt to address these problems and breathe new life into the concept of notice-and-choice.

In Part II of this Essay, we provide an overview of the general goals and approach of the *Principles*. In Part III, we provide a section-by-section overview of the *Principles*, highlighting the most notable elements of each section and explaining choices made. In Part IV, we provide the full black letter text of the *Principles*.

I. THE GOALS AND APPROACH OF THE ALI PRINCIPLES OF LAW, DATA PRIVACY

A. The Origins of the Project

We began the project in the summer of 2012. The ALI's motivation to start this project was due to a void in U.S. data privacy law. Courts, legislatures, and policymakers were struggling to understanding concepts such as the meaning of "personal identifiable information," the nature of a privacy harm, the elements of meaningful consent, and the duties that should be owed a person whose personal information is processed, among other themes. Consistency and comprehensiveness were sorely lacking in U.S. privacy law.

As the selected Reporters for a then inchoate ALI privacy project, we proposed more than a dozen possible topics and provided background on each. On September 28, 2012, we held our first meeting about this project in San Francisco. On that day, we led a discussion with a remarkable array of experts. Among the 35 attendees were judges from federal and state courts; an FTC commissioner and FTC director of a key division for privacy regulation; advocates from privacy NGO's; chief privacy officials and lawyers from a number of prominent information technology companies, including entities based in Silicon Valley; and attorneys specializing in privacy and data

---

10 (2014).

[27] On the reliance on ineffective "idealized consent," see Schwartz & Peifer, *Transatlantic Data Privacy Law*, supra note 19, at 149-50.

security law. Also in attendance was a former General Counsel of the National Security Agency and a prominent Assistant U.S. Attorney. Finally, the discussion benefited from the participation of numerous academic experts in this field, including the then Dean of the Yale Law School.

There was considerable consensus at this meeting that U.S. law would benefit from significant guidance about data privacy, and that a wide-ranging project in this area by the ALI would be a valuable undertaking. We decided to develop a new project to address the most important and vexing privacy problem of the 21st century—the vast collection, use, and disclosure of personal data by a wide array of entities. As for the section of the Restatement Second of Torts devoted to the privacy torts, we decided that while it would benefit from being revisited, this endeavor was not the most important and pressing issue for data privacy law. Moreover, the topic of the privacy torts did not fit well within our proposed project. There was also widespread consensus that we should break new ground for the ALI and tackle issues that specifically relate to data processing and information use rather than tidy up the classic issues of tort privacy.

B. The Fair Information Practice Principles (FIPPs)

We began by organizing the project around key Fair Information Practice Principles (FIPPs).[28] The FIPPs are a set of principles about the responsibilities and obligations for entities when collecting and using personal data. They also provide the rights that people should have regarding their data. A set of FIPPs were articulated in the U.S. as early as 1973 in a report by the U.S. Department of Health, Education, and Welfare (HEW).[29] The FIPPs have been restated and expanded a number of times. The Organisation for Economic Co-operation and Development (OECD) Guidelines of 1980 (updated in 2013), have included the most widely-used set of FIPPs in world

[28] FIPPs are sometimes also referred to as Fair Information Practices (FIPs).

[29] U.S. Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems 41-42 (1973).

regulation.[30] The EU Data Protection Directive and GDPR are also grounded on the FIPPs, as is the Asian-Pacific Economic Cooperation (APEC) Privacy Framework of 2004.[31] Nearly every privacy statute rests on one or another of these articulations of FIPPs.

Although the FIPPs form the backbone of privacy law in the United States and around the world, and although there is fairly widespread agreement about them, privacy laws diverge significantly in their effectiveness and scope. The FIPPs alone are open-ended; they are but a skeleton, and meaningful regulation requires more detail. In the United States, the FIPPs have often been embodied in laws in a scaled-down version – the notice-and-choice approach. One of us has critiqued this approach as one based on privacy policies that are incomprehensible to most people.[32] Another of us has critiqued the approach as failing because people cannot self-manage their privacy because it is too vast and time-consuming to do as well as too complicated to assess the costs and benefits of making choices about how and when to share their data.[33] As a consequence of the accepted, watered-down versions of the FIPPs in the United States, many other scholars have criticized the FIPPs approach to protecting privacy as inadequate.[34]

In our view, however, the problem with existing data privacy law is not with the FIPPs; rather, it is in the approach of what one of us has called "privacy self-management."[35] Although the FIPPs have certain components that involve privacy self-management, the FIPPs also have accountability principles that place obligations on organizations regarding how they use personal data. Moreover, the FIPPs already form the foundation of much privacy law, and, as a consequence, they represented the best place to focus the ALI project. What is needed, and what the *Principles* aim to supply, is sufficient guidance to bring

---

[30] OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980, expanded in 2013).
[31] GDPR, supra note 15; Asia-Pacific Economic Cooperation, APEC Privacy Framework, 2004/AMM/014rev1 (Nov. 2004); Directive, supra note 13.
[32] Schwartz & Peifer, *Transatlantic Data Privacy Law*, supra note 19, at 149-50.
[33] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. Rev. 1880 (2013).
[34] Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 Md. L. Rev. 952 (2017).
[35] Solove, *Privacy Self-Management*, supra note 33, at 1895.

more substance, uniformity, and clarity to the law. Beyond the FIPPS, we drew upon countless privacy laws, regulations, enforcement actions, and cases for ideas and approaches.

Our goal was to produce a balanced compromise, an approach to advance U.S. privacy law significantly while still maintaining fidelity to its foundations. The GDPR cannot merely be transferred to the U.S. There are some fundamental differences that make reaching consensus about certain elements of the GDPR difficult or that even make it incompatible with existing U.S. law. In our view, the *Principles* are a step forward that will be useful to legislatures working on privacy legislation, to policymakers evaluating tradeoffs in this area, and to everyone who is concerned about privacy law.

II. AN OVERVIEW OF THE *PRINCIPLES*

A. Chapter 1: Purpose, Scope, and Definitions

Section 1: Purpose and Scope of the Data Privacy Principles

The *Principles* are designed to cover organizational activities rather than personal ones. We thus focus on covering "the sale and provision of goods or services" and "the functioning of institutions and organizations, including the employment of persons."[36] The *Principles* explicitly exclude personal-data activities involving, or intended to involve "purely interpersonal or household relationships" and "personal activities." Otherwise, a person's contact list would be covered by the *Principles*; so would information that parents maintain about their children; so would anything about other individuals that people would write in their diaries. As we note in a comment: "When one individual gossips about another in a blog, for example, this situation is ill-suited for the responsibilities assigned to the data user in these Principles—such as providing notice and access—and for the rights provided to individuals in these Principles. Tort law and sometimes even criminal law are better at dealing with these situations."[37]

---

[36] Principles of Law, Data Privacy §1 comment (c).
[37] Principles of Law, Data Privacy §1 comment (f).

Also excluded from the *Principles* are "intelligence and law-enforcement activities" and "activities relating to the administration of the judicial system." These exceptions are made because these contexts are significantly different from those of businesses and other organizations.[38] Of course, many of the provisions in the *Principles* could apply to these contexts, and we encourage law enforcement entities and the judicial system to follow the *Principles* when possible. Finally, we included two exceptions to address potential conflicts with the First Amendment.[39]

Section 2: Definitions

We use much of the same terminology as the GDPR, including *data subjects*, *data controllers*, and *data processors*. We do so, first, because the United States lacks consistent terminology in its law. We also use the EU terminology because the GDPR has made EU terms widely known in the United States.[40] Additionally, using the same terminology better harmonizes U.S. and EU privacy law, as well as U.S. law and that of other nations. An important goal for this project is to achieve greater consistency between U.S. privacy law and the privacy law around the world.

We also use the term "personal data" for the type of information covered by the *Principles*. All privacy laws are limited to covering personal data rather than reaching information itself, or else these laws would regulate everything ever said or written, including every fact in the encyclopedia.[41] The definition of personal data thus fixes the scope and boundaries of privacy statutes and regulations.

The term "personal data" is used in the GDPR as well as in its predecessor, the EU Data Protection Directive.[42] In U.S. law, various

---

[38] In 1972, for example, the Supreme Court noted the special issues related to electronic surveillance in internal security matters. United States v. United States District Court (The *Keith* Case), 407 U.S. 297 (1972).
[39] Principles of Law, Data Privacy §1(b)(2)(E) & (F).
[40] Schwartz, *Global Data Privacy Law*, supra note 2, at --.
[41] Paul M. Schwartz & Daniel J. Solove, *The PII Problem*, 86 N.Y.U. L. Rev. 1814, 1866 (2011).
[42] Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the U.S. and*

terms have been used to refer to the personal data covered by privacy laws: consumer proprietary network information (CPNI) in telecommunications laws, protected health information (PHI) in HIPAA, education records in FERPA, and so on.[43] Generally, the terms "personal information" or "personally identifiable information" (PII) have been used in the United States.[44] Although there is no single term for personal data in the U.S., the most popular term thus far has been PII.[45] However, we use the term "personal data" in order to harmonize to the greatest extent possible U.S. law with privacy law worldwide.

Beyond these issues of nomenclature, the definition of PII or personal data is also one that lacks uniformity in privacy laws in the United States. In many U.S. privacy laws, definitions of PII or personal data focus primarily on data that is identified to an individual. In contrast, in the EU, personal data is defined as data that relates to an identified *or identifiable* individual.[46] *Identifiable* means that an individual might not currently be identified but could be identified by combining various pieces of data.[47] For example, an IP address is often not identified to an individual, but sometimes can readily be linked to an individual with additional data. Thus, under EU law, IP addresses are *identifiable* to individuals.[48]

Although the term PII includes the word "identifiable," in definition and practice, many U.S. privacy laws do not extend to data that are merely identifiable, but do not yet relate to an identified person. In the last decade, however, the concept of identifiable data has been taking root in the United States. As an example, in its 2012 report, *Protecting Privacy in an Era of Rapid Change*, the FTC stated

---

EU, 102 Cal. L. Rev. 877, 882-886 (2014).
[43] Id. at 887-90.
[44] Id. at 890.
[45] Id.
[46] Id. at 885-86.
[47] Id. at 886.
[48] The European Court of Justice (CJEU) has also found that IP address are "personal data" under certain circumstances, see CJEU, Case 582/14 – Patrick Breyer v. Germany (2016), at http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1116945.

that its proposed framework applies to "consumer data that can be reasonably linked to a specific consumer, computer, or other device."[49] It held that "the traditional distinction between PII and non-PII has blurred and that it is appropriate to more comprehensively examine data to determine that data's privacy implications."[50] Newer privacy laws such as the California Consumer Privacy Act (CCPA) use a definition that includes identifiable data.[51] Thus, the clear trend and contemporary approach is to define personal data to include identifiable data, and we have done so. The *Principles* thus define "personal data" as "any data that is identified or identifiable to a specific living individual."[52] This definition is similar to that of the GDPR.

We diverge from the GDPR in one key respect. Under the GDPR, identified and identifiable data are treated the same. The *Principles* treats these categories of personal data differently: "When data is identifiable, it is personal data under the Data Privacy Principles and is subject to some of the Principles but exempt from others."[53] We opted for this approach because certain principles are not as relevant and do not work as well with identifiable data. As we noted in a comment:

> Certain Data Privacy Principles are not relevant or helpful when personal data falls into the identifiable category; indeed, certain Data Privacy Principles might undermine the privacy protection of such personal data by requiring personal data to be identified in order to comply with the Principles. For example, providing individuals with access rights to their personal data requires that the data be identified to them. The Data Privacy Principles encourage that data be kept in

---

[49] FTC, Protecting Consumer Privacy in an Era of Rapid Change 18 (March 2012).
[50] Id. at 19.
[51] CCPA, Cal Civ. Code 1798.140(o)(1). For a discussion, see LOTHAR DETERMANN, CALIFORNIA PRIVACY LAW: SUPPLEMENT TO 3RD EDITION 4 (2019).
[52] Principles of Law, Data Privacy §2(b).
[53] Principles of Law, Data Privacy §2(b).

> identifiable form, rather than identified form, when possible. Regulating identified and identifiable data the same way not only removes any incentive to avoid keeping data in identified form, but also, arguably, forces the maintaining of data in the state of being identified.[54]

Our approach encourages organizations to avoid maintaining personal data in identified form. This strategy is in contrast with those privacy laws that will force organizations to identify personal data in order to administer privacy rights. That approach is counterproductive as it will increase rather than limit the possible threat to individual privacy.

B. Chapter 2: Data Privacy Principles

Section 3: Transparency Statement

Countless privacy laws require entities to have a privacy policy or notice which explains to individuals the personal data that the entity collects and how the entity uses and shares that data.[55] This perspective emerged in the mid-1990s in the U.S. when the modern commercial Internet was developing. U.S. privacy law coalesced around this standpoint, which became known as the "notice-and-choice" approach.

There are two key dimensions that underpin notice-and-choice. The first dimension is that this approach is significantly self-regulatory. Organizations are the ones that define their own rules for how they will collect, use, and share data.[56] Organizations are the ones that decide the choices given to people.[57] Under this approach,

---

[54] Principles of Law, Data Privacy §2 comment (c). For a further elaboration of our rationale, see Schwartz & Solove, *PII Problem*, supra note 41, at 880.
[55] For a discussion of this trend, see Schwartz & Peifer, *Transatlantic Data Privacy Law*, supra note 19, at 148-50.
[56] Id. at 150.
[57] HOOFNAGLE, supra note 26, at 366.

organizations have significant freedom to do what they want with the main limitation being to adhere to what they declare about their practices in the notice.

The second dimension is what one of us terms "privacy self-management."[58] The onus is placed on individuals to manage their own privacy by reading notices and making choices. As privacy's leading regulator, the Federal Trade Commission (FTC), has stated, the goals are to "[m]ake information collection and use practices transparent" and to provide people with "the ability to make decisions about their data at a relevant time and context."[59]

The problems with the notice-and-choice approach are legion and the approach has been extensively criticized. Hardly anyone actually reads privacy notices.[60] And the few people who actually try to read privacy notices will struggle to comprehend the long dense legalistic prose of these policies.[61] The choices that people can exercise are also severely limited.[62] Privacy self-management does not scale; people lack the time to review the privacy notices of every organization with which they interact. Moreover, people lack the knowledge to make meaningful cost-benefit decisions involving their data.[63]

The EU's GDPR largely rejects the notice-and-choice approach, though elements of this approach still can be found in some form in the GDPR.[64] The general approach of the GDPR, however, is quite different from notice-and-choice.

Although both of us have strongly criticized the notice-and-choice approach, we conclude that moving away from it would be too drastic a paradigm shift for U.S. privacy law and would likely undermine the

---

[58] Solove, *Privacy Self-Management and the Consent Dilemma*, supra note 33, at 1990.
[59] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change, at i (2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.
[60] Florian Schaub, Rebecca Balebako, and Lorrie Faith Cranor, *Designing Effective Privacy Notices and Controls*, 21 IEEE Internet Computing 70 (2017).
[61] Ted Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 Minn. L. Rev. 1219, 1230-32 (2002).
[62] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1609 (1999).
[63] Solove, *Privacy Self-Management*, supra note 33, at 1897.
[64] Schwartz & Peifer, *Transatlantic Data Privacy Law*, supra note 19, at 142-44.

reception of the *Principles* in the U.S. We thus opted to breathe new life into the notice-and-choice approach with several innovations aimed at correcting some of the defects of this approach. Perhaps the most important of these innovations is to bifurcate notice into two separate statements.

We drew this distinction because the current approach with privacy notice seeks to achieve two goals that are in tension with each other: (1) to inform people about how their data is used and shared; and (2) to enable regulators, policymakers, and experts to determine whether an organization's practices are appropriate and whether the organization is following the promises in their notices.[65] The tension arises because many non-expert individuals can only comprehend and digest short and simple privacy notices. Such brevity and simplicity will often omit the details that regulators, policymakers, and experts need to evaluate what the organization is doing. The "fundamental dilemma of notice" is a choice between either "making it simple and easy to understand" or "fully informing people about the consequences of giving up data, which are quite complex if explained in sufficient detail to be meaningful."[66]

We thus decided to bifurcate transparency and individual notice because these two things have different purposes, which are not fully consistent with each other. The transparency notice of Section 3 of the *Principles* aims to provide sufficient information for organizations to be accountable to regulators, policymakers, and experts. It requires that data controllers and data processers "clearly, conspicuously, and accurately explain the data controller or data processor's current personal-data activities."[67]

Section 4: Individual Notice

Standing alone from the transparency statement, the individual notice requirement of the *Principles* seeks to inform individuals about how their personal data is being collected, used, and shared. Individual

---

[65] For a discussion, see Principles of Law, Data Privacy §3 comment a.
[66] Solove, *Privacy Self-Management*, supra note 33, at 1992.
[67] Principles of Law, Data Privacy §3(b).

notice struggles to work effectively for the reasons we describe above. We thus attempt to improve how individual notice works.

To make individual notice more meaningful, the *Principles* create two levels of notice – ordinary notice and heightened notice. Heightened notice is not currently required by many privacy laws,[68] but it is important for notice to be meaningful. The *Principles* provide that heightened notice "shall be made more prominently than ordinary notice and closer in time to the particular data activity." The *Principles* define the trigger for heightened notice as follows:

> For any data activity that is significantly unexpected or that poses a significant risk of causing material harm to data subjects, the data controller should provide reasonable "heightened notice" to affected individuals. A significantly unexpected data activity is one that a reasonable person would not expect based on the context of personal-data activities. A significant risk may exist with a low likelihood of a high-magnitude injury or with a high likelihood of a low-magnitude injury. For a major potential injury, even a small likelihood may be a risk worthy of concern.[69]

The idea behind heightened notice is that notice is most necessary when the collection, use, or disclosure of personal data is potentially harmful to people or is significantly outside the norm. Heightened notice should be more conspicuous, such as a "pop up" that appears at the moment a data activity is about to occur.[70]

The timing and method of heightened notice will make it more relevant to individuals, pointing out to them when they should most be paying attention. Otherwise, important information about privacy will be drowned out in the oceans of privacy notices through which

---

[68] See Principles of Law, Data Privacy §4, Reporter's Note 6.
[69] Principles of Law, Data Privacy §4(e).
[70] See M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027 (2012) (arguing that policymakers should use "innovative new ways to deliver privacy notice" and that privacy notice should be made in a more "visceral" way).

consumers must sift. Heightened notice serves to lower the information burdens of mandated privacy disclosures. As Omri Ben-Shahar and Carl Schneider have noted, "[P]eople strip away information to make choices manageable."[71] Moreover, the privacy practices of many organizations are quite similar in many respects, and basic norms of data processing have emerged, so individuals are best informed when there are practices outside the norm or practices that could potentially harm them.[72]

We believe that our approach to notice, while different from the traditional approach in the U.S., is still quite consistent with U.S. privacy law. Bifurcating transparency and notice as well as creating two levels of notice will not solve all of the problems with notice-and-choice, but it will help significantly with its major shortcomings.

Section 5: Consent

A core element of privacy laws is consent. In the U.S., an emphasis on notice is also accompanied by a strong reliance on the affected party's consent to data processing.[73] The OECD's FIPPs also contain a concept of consent as does the EU's GDPR.[74] As a general matter,

---

[71] BEN-SHAHAR & SCHNEIDER, supra note 26, at 10.

[72] For a FTC privacy enforcement action that points in this direction, see In re Sears, In re Sears, Complaint, FT File No. 082 3099, http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf (2009); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Columbia L. Rev. 583, 634-36 (2014); Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 Nw. J. Tech. & Intell. Prop. 1, 5 (2009).

[73] See, e.g., the Privacy Act, which prohibits the disclosure of records without the "consent" of the individual, 5 U.S.C. § 552a(b), and the Health Insurance Portability and Accountability Act (HIPAA) and its requirement of patient "authorization" before release of protected health data, 45 C.F.R. § 164.508(a)(1).

[74] See OECD Privacy Principles, Principle 1 ("There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."); GDPR, supra note 15, at Art. 7 (setting out the requirements for valid consent). On the GDPR's strict restrictions placed on consent as a lawful basis for data processing, see Schwartz & Peifer, *Transatlantic Data Privacy*, supra note 19, at 143-45.

however, the U.S. relies far more heavily on the data subject's agreement to justify data processing than the EU.[75]

In the United States, there are divergent approaches to consent. A common approach is to view people's failure to opt out of various forms of data activities as a form of consent.[76] In contrast, other U.S. laws require people to affirmatively opt in to a data activity.[77]

The GDPR's approach to consent is to require affirmative consent – equivalent to opt in.[78] Opt out is not valid consent under the GDPR. As for opt out under U.S. law, where the law sometimes permits it, this approach is problematic because people often do not read or understand privacy notices.[79] Nevertheless, we aimed to avoid radically altering the approach to consent under U.S. privacy law.

The *Principles* provide that the "form by which consent is obtained must be reasonable under the circumstances, based on the type of personal data involved and the nature of the personal-data activity. The form by which consent is obtained shall reflect the expectations of the reasonable individual."[80] The *Principles* do not embrace either opt out or opt in; instead, consent is left deliberately open-ended so the standard can evolve situationally and contextually.

In at least one way, we have tightened up consent. According to the *Principles*:

> In situations in which heightened notice is required pursuant to Principle 4, only clear and affirmative consent shall suffice for valid consent. Clear and affirmative consent cannot be inferred from inaction.[81]

---

[75] For a discussion of "idealized consent" in the U.S. legal privacy regime, see Schwartz & Peifer, *Transatlantic Data Privacy*, supra note 19, at 149-50.
[76] See, e.g., the Gramm-Leach-Bliley Act, 15 U.S.C. § 6802.
[77] See, e.g., the Fair Credit Reporting Act, 15 U.S.C. § 1681b(a)(3)(F) (2012).
[78] GDPR, supra note 15, at Art. 7. The Article 29 Working Party of the EU has provided an extensive guideline on interpreting consent under the GDPR. Article 29 Working Party, Guidelines on consent under Regulation 2016/679 (Adopted on 28 November 2017, as last Revised and Adopted on 10 April 2018).
[79] Schwartz, *Privacy and Autonomy in Cyberspace*, supra note 62, at 1634.
[80] Principles of Law, Data Privacy §5(f).
[81] Principles of Law, Data Privacy §5(f).

Accordingly, in situations involving data activities that are unexpected or that are potentially harmful, affirmative opt-in consent is required. Our approach avoids the tsunami of opt in consent requests that this legal requirement might otherwise provoke.[82] Such opt in requests can quickly become meaningless and annoying when people are bombarded with them about matters that are rather trivial.

Section 6: Confidentiality

The principle of confidentiality is oddly often not explicitly included in the FIPPs or many privacy laws, though it is clearly implied and is a byproduct of the FIPPs.[83] The *Principles* include an explicit section on confidentiality. The *Principles* recognize duties of confidentiality when there is "an express or implied promise of confidentiality or a legal obligation of confidentiality."[84] The *Principles* also recognize a duty of confidentiality under the following circumstances:

> Confidentiality should also apply to situations in which entities (i) hold themselves out to be privacy-respecting to gain trust of individuals who use their product or service, and (ii) cause individuals to reasonably believe that the entity will not disclose their personal data based on reasonable social expectations. Such reasonable belief can be based on privacy norms, or established practices.[85]

---

[82] The GDPR guards against this risk largely by heightening the requirements for consent to be valid, and thereby making it a relatively unattractive path for justification of legal processing. The guidance of consent from the United Kingdom's Information Commissioner's Office (ICO) demonstrates this tendency. ICO, Lawful basis for processing: Consent (March 22, 2018), at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/

[83] Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 Geo. L.J. 123, 181-82 (2007)

[84] Principles of Law, Data Privacy §6.

[85] Principles of Law, Data Privacy §6.

By adding confidentiality to the FIPPs, the *Principles* close an important gap in U.S. privacy law.

Section 7: Use Limitation

A fundamental difference between the United States approach and that of the EU is that the EU requires a lawful basis for the processing of personal data.[86] This requirement is anchored at the constitutional level in the EU.[87] The U.S. does not generally require a justification to process personal data; indeed, through the First Amendment, as interpreted by courts, its data privacy law features strong protection for a free flow of information.[88] In the U.S., the law regulates and restricts a processing of personal data primarily when this activity might cause harm.

We conclude that a general departure from this aspect of United States privacy law would make the *Principles* too fundamentally different from the existing United States law. In biology and law, transplants work best if compatible with a host organism.[89] Our goal is to find an approach that would not break radically from existing concepts in United States law.

Although the *Principles* do not use the lawful basis approach for the initial collection of personal data, we followed this approach for secondary uses of personal data. A secondary use of personal data is one "unrelated to those stated in the notice to individuals pursuant to Principle 4 without the consent of the individuals."[90] For such uses, an initial consent to use the data does not exist, so greater limitations should be placed on such unrelated processing. It is here where the idea of a lawful basis to process personal data, such as found in the GDPR, fits quite well. Principle 7 calls for either consent by the data subject

---

[86] CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION 242 (2d ed. 2007).
[87] Schwartz & Peifer, *Transatlantic Data Privacy*, supra note 19, at 123-27.
[88] Id. at 134-36.
[89] In the comparative law literature, this idea is that of an appropriate "fit" between a law and a recipient culture. Like much else in comparative law, the concept is not uncontested. See, e.g., Michele Graziadei, *Transplants and Receptions*, in THE OXFORD HANDBOOK OF COMPARATIVE LAW 441, 472-73 (Mathias Reimann & Reinhard Zimmermann, eds. 2006).
[90] Principles of Law, Data Privacy §7.

or the fulfillment of the Principle's exceptions for consent. These exceptions include the fulfillment of a contract to which the data subject is a party; the significant advancement of the protection of health or safety of the data subject or other people; and, as in the GDPR, a catch-all for serving a "significant legitimate interest" without "posing a significant risk of material harm to the data subject or others" and without being "significantly unexpected."[91]

Section 8: Access and Correction

The *Principles* include a right for individuals to access their personal data and request corrections of errors. This is a common set of rights in privacy law, and our approach does not go in any dramatically new direction. At the same time, we were careful to strike a balance between the interests of data processors and data subjects. As one example, data processors need only provide "reasonable process to challenge the accuracy of a data subject's personal data."[92] It is left for legislatures and courts to further define, in different contexts and circumstances, the kind of process that meets this reasonableness standard. As a further example, a data subject need only provide "a reasonable basis in proof" to demonstrate that stored data is incorrect.[93] Here, too, we use a reasonableness standard under the logic of reciprocal treatment. Or as the saying goes, "What is sauce for the goose is sauce for gander."

Section 9: Data Portability

More recent privacy laws are including a right to data portability. Such a right is included in the GDPR as well as in California's CCPA.[94] We included such a right in the *Principles* as well. It remains to be seen in practice whether the right to data portability emerges into a meaningful right.

There are many challenges in porting data from a platform as one individual's personal data might be intertwined with the personal data

---

[91] Compare GDPR, Art. 6(1)(f) with Principles of Law Data Privacy §5(i).
[92] Principles of Law, Data Privacy §8(e)(1).
[93] Principles of Law, Data Privacy §8(e)(2).
[94] GDPR, supra note 15, at Art. 20; CCPA, Cal. Civ. Code §1798.100(d).

of others. This combination of data can impinge upon the privacy of such third parties. Yet, redaction of this information to exclude the intermingled personal data of other individuals might affect or even change its meaning because the context has been altered. For example, on a social media site, a person may have commented on the posts of others. These comments might lose their meaning when separated from the posts of the other users. We decided not to tackle these issues, as the right to data portability is in its infancy, and more time and experience are needed to hone this right.

Section 10: Data Retention and Destruction

According to the *Principles*, "Personal data that no longer serves the uses identified in the notice that was provided or other legitimate interests shall be destroyed using reasonable procedures to ensure that it is unreadable or otherwise indecipherable."[95] Data destruction is a long established principle in U.S. privacy law. For example, the Fair Credit Reporting Act authorizes a set of federal agencies to regulate the destruction of consumer data from consumer reports.[96] Drawing on this authorization, the FTC has issued a Disposal Rule for those entities over which it has regulatory power.[97]

More complicated than this notion of data destruction is the thorny concept of data retention. U.S. law generally acknowledges ongoing legitimate business needs, legal obligations, and archival purposes as requiring the ongoing storage of personal data. The approach in the *Principles* is to establish a general rule of limits on retention ("A data controller may retain personal data only for legitimate purposes that are consistent with the scope and purposes of notice provided to the data subject.") and make it subject to carefully drawn exceptions.[98]

Finally, we did not include a right to erasure (also referred to as a "right to deletion" or a "right to be forgotten"). Such a right may find its way into U.S. law, but such an interest will need to be carefully

---

[95] Principles of Law, Data Privacy §10.
[96] 15 U.S.C. § 1681w.
[97] 16 C.F.R. § 682.
[98] Principles of Law, Data Privacy §10(a)-(d).

crafted not to run afoul of the First Amendment, which continues to evolve regarding how it interacts with restrictions on information flow of data privacy law.[99]

Section 11: Data Security

We include data security in the *Principles* because we view it as an integral part of information privacy. As we noted in a comment to the *Principles*, "Nearly every version of the FIPPs includes protections for the security of personal data. Data security is one of the most common requirements of data privacy statutes and regulations. The privacy and security of personal data are related, and they cannot exist in isolation."[100]

Our approach to data security is the reasonable safeguards approach, an approach to data security common in the United States and worldwide.[101] This approach has benefits and shortcomings. The primary benefit of this approach is that it is open-ended and evolves as standards and best practices develop and as security threats change. The shortcoming of this approach is that, left to their own devices, organizations can interpret "reasonable" in essentially unreasonable ways and fall short of what they need to do. This approach also does not provide detailed guidance to organizations about the specific security measures they should use.[102]

An alternative approach is to provide a list of specific standards, an approach embodied by the HIPAA Security Rule and some state laws.[103] The virtue of this approach is that it provides guidance and specificity; the shortcoming is that many organizations become obsessed with checking boxes on a "to do" list without paying sufficient attention to the quality of the substance of various security

---

[99] Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right To Be Forgotten, and the Construction of the Public Sphere*, 67 Duke L.J. 981 (2018).
[100] Principles of Law, Data Privacy §1 comment (c).
[101] GDPR, supra note 15, at Art. 32. For U.S. law, see the Gramm-Leach-Bliley Act, 16 C.F.R. § 314.3(a).
[102] A recent opinion of the Eleventh Circuit aired these issues regarding the necessary degree of specificity in a FTC's finding that a party committed an unfair trade practice due to a data security breach. LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018).
[103] Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. § 164.530(c)(1). Regarding such state data breach laws laws, see Schwartz & Solove, *PII Problem*, supra note 41, at 1831-34.

measures. Another shortcoming is that this approach might omit important safeguards, and if the mandated standards are not updated over time, the framework will lack new best practices and effective responses to threats. This risk of standards stagnating is a real one in today's age of legislative gridlock. We ultimately opted for the reasonableness approach because of its simplicity and ability to develop over time through input from courts and government agencies, including the FTC.

The *Principles* also include a data breach notification requirement. Data breach notification originated with a 2003 California law, and spread faster than wildfire to all 50 states in the United States as well as around the world.[104] The *Principles* define a breach broadly to include the "access, acquisition, use, modification, disclosure, or loss of personal data in an unauthorized manner that compromises the privacy or security of the personal data."[105] This broad definition is designed to avoid arbitrary limitations on what can constitute a breach. Far too often, breach notification laws get bogged down in definitions of a breach that have no relationship to the most important issue, which concerns the threat or harm that such breaches pose.[106] Our definition of a breach is similar to the one found in the HIPAA Breach Notification Rule.[107]

Many breach notification laws specify specific time periods within which to notify. Indeed, there seems to be a competition among jurisdictions to have the shortest time deadline after discovery of a breach to notify. Early notification often does not produce good information because it can take a while to understand the extent and nature of a breach. Accordingly, we opted for a more contextual approach by requiring notification "without unreasonable delay."[108]

---

[104] Cal. Civ. Code § 1798.29. Regarding the spread of data breach notification laws, it is found in the GDPR, supra note 15, at Art. 33-34.
[105] Principles of Law, Data Privacy §11(b)(1).
[106] Hence, state data breach notification statutes split on whether mere "access" to personal data can trigger a notification, or whether there must be some indication of likely harm to an individual. For an overview of these laws, see DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 189-97 (2019).
[107] HIPAA Breach Notification Rule, 45 C.F.R. § 164.404.
[108] Principles of Law, Data Privacy §11(b)(2).

Section 12: Onward Transfer

The *Principles* require reasonable due diligence to ensure that entities receiving personal data will protect it.[109] The basic idea here is that data privacy protection must follow personal data as an initial organization hires vendors, business associates, and other third parties to assist it and, as a consequence, shares the data with these other entities. Organizations use a wide array of third-party vendors to help them process personal data, and these vendors may use additional vendors for certain purposes, and the chain goes on and on.[110]

The law has begun to address these relationships, and how contracts are to play a positive role in safeguarding privacy.[111] When personal data passes through a wide network of entities, contracts must play a central role in protecting this information.[112] The *Principles* addresses the issues to be covered in the contracts between the initial data collector and the entities receiving personal data from it.

The *Principles* do not include restrictions on cross-border data transfers. First, and unlike the EU, the United States lacks a governmental entity that can make a determination of adequacy.[113] Second, the Principle's requirements for onward transfer already have requirements for companies to provide safeguards, whether such transfer is domestic or international.[114] Third, the United States

---

[109] Principles of Law, Data Privacy §12(b).

[110] As the Principles state, "Onward transfer is one of the greatest challenges to privacy protection, as accountability and control over personal data can break down as personal data is transferred along a chain of entities." Principles of Law, Data Privacy §12, comment a.

[111] HIPAA requires that there be a business-associate agreement (BAA) for onward transfers of protected health information (PHI). 45 C.F.R. § 164.502(e). HIPAA also regulates downstream personal-data transfers—when any business associate (BA) transfers personal data to another entity, that entity is deemed to be a BA too. Similarly, the Gramm–Leach–Bliley Act and its applicable regulations place numerous requirements on a financial institution concerning its selection of and use of "service providers." 15 U.S.C. § 6802(b)(2).

[112] Daniel J. Solove, *Our Privacy and Data Security Depend Upon Contracts Between Organizations*, Privacy + Security Blog (May 5, 2014), https://teachprivacy.com/privacy-data-security-depend-upon-contracts-organizations/.

[113] On the GDPR's approach, see GDPR, supra note 15, at Art. 45. On the historic background of the adequacy requirement, see Paul M. Schwartz, *The EU-US Privacy Collision*, 126 Harv. L.Rev. 1966, 1977-81 (2013).

[114] Principles of Law, Data Privacy §12(a).

government has vast surveillance powers that the law does not necessarily restrict sufficiently.[115] An adequacy requirement might lead the United States to demand much more of the rest of the world than of itself, or set the resulting bar so low as not to be meaningful. Finally, this type of restriction can readily become politicized, as is shown by the arguments in the U.S. that the EU's restrictions on data transfers to the U.S. are (barely) disguised trade protectionism.[116] Hinting as much in the antitrust context, President Barack Obama analyzed European investigations into Facebook and Google during his administration in these terms, "[O]ftentimes what is portrayed as high-minded positions on issues sometimes is just designed to carve out some of their commercial interests."[117]

C. Chapter 3: Accountability and Enforcement

Section 13: Accountability

There has been a tremendous recent interest at an international level in standards of accountability for the 21st century.[118] This effort began with the Irish Data Protection Commissioner's multi-year "Galway" initiative.[119] These initial steps were followed by accountability projects led by the French data protection commissioner and a resolution on the topic issued in 2011 by EU data protection

---

[115] Comparative assessments of respective national schemes for regulation of national surveillance apparatus prove to be extremely difficult. For a comparative set of essays that evaluates the U.S. as well as other countries regarding a subset of their surveillance of private sector information, see BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA (Fred Cate & James X. Dempsey, eds., 2017). For a concise overview and critique of the U.S. system, see LAURA K. DONOHUE, THE FUTURE OF FOREIGN SURVEILLANCE (2016).

[116] Schwartz & Peifer, *Transatlantic Privacy*, supra note 19, at 157.

[117] Kara Swisher, White House. *Red Chair. Obama Meets Swisher*, RE/CODE (Feb. 15, 2015), http://www.recode.net/2015/2/15/11559056/white-house-red-chair-obama-meets-swisher [https://perma.cc/A5UX-XEES]. As noted, President Obama was speaking of EU antitrust investigations of Facebook and Google, but his observations are illustrative as well of U.S. attitutes towards European privacy activities regarding leading U.S. tech companies.

[118] The Centre for Information Policy Leadership, Data Protection Accountability: The Essential Elements; A Document for Discussion 6 (October 2009).

[119] Id.

commissioners in Madrid.[120] As a policy idea, the accountability principle focuses on whether a data processing entity has created internal processes that are commensurate with potential data threats.[121]

The *Principles* require a reasonable comprehensive privacy program which includes written privacy and security policies and procedures, personal-data inventory, risk assessment, training program, privacy and security by design, and privacy and security by default.[122] For privacy by design, the *Principles* do not specify design choices. Mandating specific technological design is quite a challenging undertaking for law,[123] and, moreover, would likely face unified and strong opposition from the tech industry. Although the law probably should do more to regulate design, we were concerned about how to do this well while also being practical about not pushing U.S. law too far.

The *Principles*, therefore, opt merely to require that "[d]esign choices and the reasoning that supports them shall be documented."[124] Policymakers, regulators, and other actors can then evaluate these decisions. We leave it up to these parties to delve into the substance of design decisions on a case-by-case basis.

At first glance, our approach might seem weak, but we believe that this viewpoint is significantly strengthened by the Principle's requirement of documentation, something that other laws often fail to require regarding privacy by design. Any organization can claim that it is practicing privacy by design, but mandated documentation forces organizations to create a record that can later be evaluated and critiqued by regulators or others. This adds accountability to the process. Documentation showing that the design process for privacy was incomplete or poorly-conceived could be damaging later on, as

---

[120] Paula Breuning, Accountability, 10 BNA World Data Protection Report 1-3 (V. 10, 2010).
[121] The Centre for Information Policy Leadership, Data Protection Accountability: The Essential Elements; A Document for Discussion, 8-9 (October 2009).
[122] Principles of Law, Data Privacy §13.
[123] Despite or perhaps due to the challenges of legal mandates for design, there has been a flurry of rewarding academic studies on this topic. See, e.g., WOODROW HARTZOG, PRIVACY'S BLUEPRINT (2018); Ari Ezra Waldman, *Designing Without Privacy*, 55 Houston L.Rev. 659, 687 (2018).
[124] Principles of Law, Data Privacy §13(d).

during a post-breach litigation. Our hope is that the documentation requirement will prevent organizations from treating privacy by design as a meaningless shibboleth and put thought and care into designing with privacy in mind.

Section 14: Enforcement

The *Principles* are purposely agnostic in this section: "To the extent that the law recognizes any remedies for these Principles, these remedies shall be effective, proportionate, and dissuasive."[125] This section goes on to list potential remedies and offer guidance, but does not mandate specific remedies for privacy violations or harms. In other words, the *Principles* offer a wide range of ingredients among which legislatures, judges, policymakers, and privacy professionals can choose. We opt for this approach because the *Principles* are designed to serve in a broad range of settings, including legislation, adjudication, and the shaping of internal policies and procedures.

In listing a broad range of these possible ingredients, or factors, for deciding whether to provide remedies, we acknowledge, moreover, that an attempt on our part to shape more definitive, or harder-edged rules, would have created significant disagreement among the Members of the ALI. Hence, we place our trust in the ability of the legal process to work out specific remedies in an evolving fashion for different data processing contexts. The important overarching goal is that remedies be "effective, proportionate, and dissuasive."[126] Regarding our list of factors, these include the gravity of the infringement, the fault of the infringer, unjust enrichment, and the "need for general deterrence" among other things.[127]

Notably, the *Principles* do not require proof of a privacy harm in order for there to be a remedy. Despite the growth of the intentional infliction of emotional distress tort and the privacy torts, courts in privacy cases still struggle to recognize that only emotional or

---

[125] Principles of Law, Data Privacy §14(a).
[126] Principles of Law, Data Privacy §14(a).
[127] Principles of Law, Data Privacy §14(c).

psychological harm should form a basis for a lawsuit. Dealing with harms created by data security breaches, for example, federal appellate courts have issued a series of conflicting opinions.[128] As a further example of how courts have struggled with the proper definition of a privacy harm, in *FAA v. Cooper*, the Supreme Court held that the Privacy Act does not recognize psychological harms as solely sufficient to create an actual injury.[129] The *Cooper* Court's reluctance to find actionable harms from privacy invasions is representative beyond its particular statutory context.

Courts are also skeptical of privacy tort actions that point only to emotional or mental harms. Already in 2003, Joel Reidenberg concluded his critique of privacy enforcement actions by warning, "privacy remedies for personal wrongs are not easily accommodated within the existing set of legal rights."[130] A similar negative judgment can be reached today. Too often, courts only recognize a narrow range of privacy harms and leave plaintiffs without a remedy.[131]

III. THE BLACK LETTER OF THE ALI PRINCIPLES OF LAW, DATA PROTECTION

This Part presents the complete black letter for the *Principles of Law, Data Protection.* The entire *Principles* project is more than 100

---

[128] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 Tex. L. Rev. 737 (2018).

[129] FAA v. Cooper, 132 S. Ct. 1441, 1453 (2012) ("[T]he term 'actual damages' can include nonpecuniary loss. But this generic meaning does not establish with the requisite clarity that the Privacy Act, with its distinctive features, authorizes damages for mental and emotional distress.").

[130] Joel Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 Hastings L.J. 877, 892 (2003).

[131] For example, federal circuit courts are divided over on the issue of whether an increased risk of a pecuniary harm like identity theft, or reasonable expenditures to avoid such harms, are injuries giving rise to Article III standing. Compare the expansive holdings in Galaria v. Nationwide Mut. Ins., 663 F. App'x 384, 388 (6th Cir. 2016); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 967, 969 (7th Cir. 2016); Krottner v. Starbucks Corp., 628 F.3d 1139, 1140-1143 (9th Cir. 2010); Attias v. Carefirst, Inc., 865 F.3d 620, 626-629 (D.C. Cir. 2017), with the narrow holdings on the harm issue in Katz v. Pershing, 672 F.3d 64, 79-80 (1st Cir. 2012); Reilly v. Ceridian Corp., 664 F.3d 38, 40, 43 (3d Cir. 2011); Beck v. McDonald, 848 F.3d 262, 273-277 (4th Cir. 2017). For an analysis of how these cases handle the issue of privacy harm, see generally Courtney M. Cox, *Risky Standing: Deciding on Injury*, 8 Ne. U. L.J. 75 (2016) (placing the cases in a conceptual framework).

pages and includes illustrations, commentary, and reporters' notes. It can be obtained from the ALI at https://www.ali.org/.

Chapter 1: Purpose, Scope, and Definitions

§ 1. Purpose and Scope of the Data Privacy Principles

(a) *Purpose of the Principles.* The Data Privacy Principles cover some, but not all, data activities regarding personal data. The Data Privacy Principles are designed to inform the development of best practices, to bring coherence to existing law, and to guide the development of emerging law. These Principles can serve as the framework for laws, a data-privacy model code, or industry-specific codes.

(b) Scope

(1) *Covered* Personal-*Data Activities.* These Principles cover personal-data activities involving, or intended to involve:

(A) the sale and provision of goods or services; and

(B) the functioning of institutions and organizations, governmental, for-profit, and nonprofit, and natural persons. including the employment of persons.

(2) *Personal-Data Activities Not Covered.* The Data Privacy Principles do not cover personal-data activities involving, or intended to involve:

(A) purely interpersonal or household relationships;

(B) personal activities;

(C) activities relating to national intelligence and law-enforcement;

(D) activities relating to the administration of the judicial system, including judicial matters;

(E) communications seeking to promote public understanding or discussion, or data activities that are intended to support such communications, including data activities connected with libraries, archives, journalism, public commentary, scholarship, blogging, biography, satire, or the arts; or

(F) the public exchange of publicly available information, except insofar as such exchange is made for particular purposes that would justify the application of these Principles and is consistent with the First Amendment.

§ 2. Definitions

(a) *Data.* "Data" means information recorded in any form or medium.

(b) *Personal Data.* "Personal data" means any data that is identified or identifiable to a specific living individual.

(1) Data is "identified" when it is directly linked to a natural person, or when there is a high probability that it could be linked to a specific person. When data is identified, it is personal data under the Data Privacy Principles and is subject to all relevant Principles.

(2) Data is "identifiable" when there is a moderate probability that it could be linked to a specific person by the intended recipient(s) or by others reasonably foreseeable to have access to the data. When data is identifiable, it is personal data under the Data Privacy Principles and is subject to some of the Principles but exempt from others.

(3) Data is "nonidentifiable" when there is a low probability that it could be linked to a specific person. Such data is not personal data under these Data Privacy Principles.

(4) Data controllers and data processors are under a continuing obligation to engage in reasonable measures to review their activities for circumstances that may have altered the ability to identify a specific person. If a data controller or data processor finds that information previously classified as nonidentifiable is actually identified or identifiable, it is obligated to change its handling of this information so as to comply with these Principles.

(c) *Data Subject.* A "data subject" is a natural person to whom the personal data relates.

(d) *Personal-Data Activities.* A "personal-data activity" is any of the activities:

(1) "Collection" means the acquisition of personal data either directly from the individual or from other sources, including a third party.

(2) "Access" means the retrieval or viewing of personal data by the person who initially collected it, or by another person.

(3) "Retention" means the maintenance or storage of personal data.

(4) "Use" means the processing of personal data or the making of decisions based in whole or in part on that personal data.

(5) "Sharing" means providing others with personal data or with access to personal data.

(6) "Destruction" means disposing of, or deleting, personal data in a manner that makes it permanently incomprehensible.

(e) *Data Controller.* A "data controller" is any person, organization, or agent thereof that engages in any covered personal-data activity and that determines the purposes of such activity.

(f) *Data Processor.* A "data processor" is any person, organization, or agent thereof that engages in any covered personal-data activity on behalf of a data controller or another data processor.

Chapter 2: Data Privacy Principles

§ 3. Transparency Statement

(a) *Requirement.* A data controller or data processor that engages in a personal-data activity shall provide a publicly accessible transparency statement about these activities.

(b) Content

(1) The transparency statement shall clearly, conspicuously, and accurately explain the data controller or data processor's current personal-data activities.

(2) When the law requires or permits a data controller or data processor to withhold certain information, such as trade secrets or confidential information, the transparency statement need not include this information.

(c) *Accessibility.* The transparency statement shall be reasonably accessible to any interested person. In the event that the transparency statement is changed, previous versions of the statement shall be retained and reasonably accessible.

(d) *Proportionality.* A transparency statement is required for both identified and identifiable personal data. The detail and sophistication of the transparency statement shall be proportionate to the magnitude of the privacy and security risks of the personal-data activities.

§ 4. Individual Notice

(a) Requirements for individual notice

(1) A data controller that engages in a data activity involving identified personal data that implicates a data subject's interests, as recognized by these Data Privacy Principles, shall provide notice

individually to that data subject. This notice shall fulfill the requirements of subsection (d) below.

(2) The individual notice shall be distinct from the transparency statement required in § 3 and provided in addition to the transparency statement.

(3) All aspects of the notice should be provided as reasonably practicable. A data controller's capabilities and resources are factors in determining whether providing certain aspects of notice is reasonably practicable.

(4) Individual notice need not be provided when personal data is only identifiable, but not yet identified.

(b) *Accessibility*. The notice shall be reasonably accessible to the data subject.

(c) *Timing of notice.* The notice shall be provided to the data subject at an appropriate time that will enable the data subject to exercise interests recognized by these Data Privacy Principles.

(d) Content of notice

(1) The notice shall be clear and intelligible to a reasonable person.

(2) The notice shall inform the data subject of the nature of the data activity, the uses made of the data, the interests implicated, and how the data subject may exercise those interests.

(3) The notice shall inform the data subject of any rights provided by applicable law that are relevant to the data activities in which the data controller is engaging.

(4) The notice shall contain information enabling the data subject to contact the data controller with questions or complaints about the data controller's data activities. When a data subject contacts the data controller in the described manner, the data controller shall respond as soon as reasonably practicable.

(e) Heightened notice

(1) For any data activity that is significantly unexpected or that poses a significant risk of causing material harm to a data subject, the data controller should provide reasonable "heightened notice" to the data subject.

(2) A significantly unexpected data activity is one that a reasonable person would not expect based on the context of the personal-data activities.

(3) A significant risk may exist with a low likelihood of a high-magnitude injury or with a high likelihood of a low-magnitude injury. For a major potential injury, even a small likelihood may be a risk worthy of concern.

(4) Heightened notice shall follow all of the requirements of notice specified above, as well as additional requirements specified in this subsection.

(5) Activities regarding personal data are "significantly unexpected" when they are at substantial variance with the expectations of a reasonable person.

(6) Material harm exists when a reasonable person would recognize that a data subject may suffer financial loss, reputational damage, embarrassment, emotional distress, chilling of activities protected under federal or state constitutional law, or from revelations of personal data that the data subject wants to conceal.

(7) Heightened notice shall be made more prominently than ordinary notice and closer in time to the particular data activity.

(f) *Material changes in policies and practices.* Additional notice shall be provided to a data subject when a data controller makes any material change in its policies and practices with respect to personal data.

(g) *Exceptions to individual notice.* A data controller may refrain from providing notice if there is no reasonably practicable way to inform the data subject. The data controller shall document why providing notice is not reasonably practicable and include this information in the transparency statement in § 3. This statement should also be publicized on the data controller's website home page or through other reasonable means.

§ 5. Consent

(a) Consent means the willingness of the data subject to permit the personal data activity in question.

(b) A data subject shall be given understandable and easy-to-use means to permit exercise of meaningful choice in relation to personal-data activities regarding the data subject's personal data.

(c) When the law requires consent of the data subject for personal data activities, or a data controller relies on the consent of the data subject as the justification for personal data activities, these principles apply in the absence of a valid exception.

(d) The data controller is responsible for obtaining consent. A data controller may contract with another entity to obtain the consent of data subjects.

(e) Consent is invalid unless the data subject is provided reasonable notice that satisfies the standards of Principle 4.

(f) Consent is invalid if it is obtained in a misleading or deceptive fashion.

(g) Form of consent

(1) The form by which consent is obtained must be reasonable under the circumstances, based on the type of personal data involved, the nature of the personal-data activity, and the understandings of a reasonable data subject.

(2) In situations in which heightened notice is required pursuant to Principle 4(e), only clear and affirmative consent shall suffice for valid consent. Clear and affirmative consent cannot be inferred from inaction.

(3) Except for paragraph (2) above, consent can be an apparent one whenever it can reasonably be understood that the individual consents to a particular use of personal data. Apparent consent occurs when words or conduct are reasonable understood by another to be intended as consent.

(h) *Withdrawal of consent.* An individual shall be permitted to withdraw consent, subject to legal or otherwise reasonable restrictions, and reasonable notice to the entity that collected the personal data.

(i) *Exceptions to the consent requirement.* Personal data activities may be conducted without consent if:

(1) the personal data activity is required by law;

(2) obtaining consent would be impermissible under law; or

(3) obtaining consent would be impractical, or too costly or difficult and the use satisfies one or more of the following criteria:

(A) the personal data activity is necessary in the performance of a contract to which the data subject is a party;

(B) the personal data activity significantly advances the protection of the health or safety of the data subject or other people;

(C) the personal data activity significantly advances protection against criminal or tortious activity by a data subject;

(D) the personal data activity significantly advances the public interest, and it would not pose a significant risk of material harm sufficient to trigger heightened notice pursuant to Principle 4(e); or

(E) the personal data activity serves a significant legitimate interest, and it neither poses a significant risk of material harm to the data subject or others, nor is significantly unexpected, as is defined in § 4(e)(1).

§ 6. Confidentiality

(a) *Duty of confidentiality.* A data controller or data processor shall maintain the confidentiality of personal data when:

(1) confidentiality is required by law

(2) confidentiality is required by ethical standards (such as professional rules of conduct); or

(3) when the personal data is collected under an express or implied promise of confidentiality.

(b) *Relationships of trust.* A data controller or data processor shall also maintain confidentiality when it (i) holds itself out to be privacy-respecting to gain the trust of data subjects who use its product or service, and (ii) cause data subjects to reasonably believe that the it will not disclose their personal data based on reasonable social expectations. Such reasonable belief can be based on privacy norms, or established practices.

(c) *Service providers and onward transfers.* An onward transfer of personal data by a data controller or data processor's to another data processor is not a breach of confidentiality if authorized by Principle 12 (onward transfer).

(d) *Breach of confidentiality.* A duty of confidentiality is not breached under the following circumstances:

(1) the data subject consents to the disclosure of personal data;

(2) disclosure is required by law, such as judicial process or a statute requiring disclosure; or

(3) disclosure is necessary for the health or safety of the data subject or other people.

Any such disclosures under these circumstances should involve only the minimum necessary personal data related to the disclosure purpose and be released only to individuals or entities that are best suited for such purpose.

§ 7. Use Limitation

(a) *Secondary uses.* Personal data shall not be used in secondary data activities unrelated to those stated in the notice required by Principle 4 without a data subject's consent. Secondary data activities are those unrelated to those stated in the notice to the individual as required by Principle 4.

(b) *Exceptions.* Personal data may be used in secondary data activities based on the exceptions to consent set out in Principle 5(i).

(c) Transparency and notice

(1) Notice of the specific justification for using data under subsections (b)(2)(D) and (E) shall be conveyed to the data subject as soon as practicable.

(2) When it is reasonably foreseeable that personal data will be used in the future in a way authorized by subsection (b), the transparency statement (Principle 3) and individual notice to data subjects (Principle 4) shall be updated to state this fact. Such additional notice shall be provided in a fashion consistent with Principle 4(f).

§ 8. Access and Correction

(a) *Information about storage of identified personal data.* A data controller must inform a data subject whether the data controller or data processor acting on behalf of the data controller stores identified personal data about the data subject. This information shall be communicated in a reasonably timely fashion after a request by a data subject who provides reasonable proof of identity.

(b) *Information about storage of identifiable personal data*. Access and correction interests do not extend to identifiable personal data.

(c) *Access.* Unless access can be refused under subsection (e) or (f), a data subject is entitled on request to access personal data about the data subject stored by a data controller or data processor acting on behalf of the data controller. A data controller must provide access or a reason for denying access within a reasonable period of time after the request is made.

(d) *Verification of identity*. When access to personal data is requested by a data subject or a person acting on behalf of a data subject, a data controller shall use reasonable means to verify the identity of the data subject or the validity of the legal authority of the person acting on behalf of the data subject before providing such access.

(e) Correction

(1) A data controller shall provide a data subject with a reasonable process to challenge the accuracy of the data subject's personal data.

(2) When a data subject provides a reasonable basis in proof to demonstrate that the data subject's personal data is incorrect, the data controller shall correct the data by amending or deleting it, or by other means. The data controller shall take reasonable steps to ensure that the errors are corrected in any copies of the personal data stored by data processors that have received it from the data controller.

(3) A data controller that rejects a data subject's contention of error shall provide a timely explanation. When reasonably practicable, the data subject may add a statement of disagreement to the record where

the data is stored. This statement shall be included when the personal data is shared with another person or entity.

(e) *Exceptions.* Access and an opportunity for correction need not be provided when:

(1) disclosure of the data subject's personal data is prohibited or restricted by law, or a duty to protect proprietary information or trade secrets;

(2) disclosure would violate the privacy of persons other than the data subject; or

(3) the balance of interests between the data controller and the data subject weighs against access and an opportunity for correction. Factors in assessing this balance include whether the burden, expense, or security risks of access and correction would be unreasonable or disproportionate to the harms to the data subject's privacy.

(f) A data controller may not provide access and opportunity for correction to a data subject when the law prohibits these interests.

§ 9. Data Portability

(a) *Data portability request and a usable format.* When a data subject makes a data portability request and when required by law, or when appropriate, reasonable, and practicable, a data controller shall provide to the data subject a copy of the data subject's personal data in a usable format. A usable format is one that is structured, commonly used, and machine-readable in a way that permits a reasonable data subject to use this information in other platforms or situations without undue burden.

(b) *Scope of portable personal data.* Portable personal data is personal data that the data subject provided to the data controller or that the data subject generated while using the data controller's services or products and that was stored by the data controller or by a data processor on its behalf.

(c) *Verification of identity and authority.* Before providing the personal data in response to a data portability request, a data controller shall use reasonable means to verify that the requestor is the data subject or a person who has legal authority to make the request.

(d) *Redaction of personal data of others.* A response to a data portability request shall redact identified and identifiable personal data about other data subjects when providing such data would violate these Principles.

(e) When appropriate, a data controller may require a reasonable fee for responding to a data portability request.

(f) If only identifiable personal data is maintained about a data subject and if complying with a data portability request would require identifying this personal data, then the data controller does not have to comply with the data portability request.

§ 10. Data Retention and Destruction

(a) *Scope of retention of personal data.* A data controller may retain personal data only for legitimate purposes that are consistent with the scope and purposes of notice provided to the data subject. A data processor shall retain personal data only as justified by its contract with the data controller or the data processor that provided the personal data and when consistent with these Data Privacy Principles

(b) *Data retention for archival or research purposes.* When personal data is stored for archival or research purposes, reasonable access limitations shall be set to protect privacy.

(c) *Destruction of personal data.* When retention of personal data is no longer permitted under subsection (a), it shall be destroyed within a reasonable time by reasonable means that make it unreadable or otherwise indecipherable. A data controller that has provided personal data to a data processor shall take reasonable steps to ensure that the data processor properly destroys the data.

(d) *Exceptions to data destruction.* Exceptions to the data-destruction requirement include:

(1) a legal obligation to retain the personal data;

(2) retaining the personal data is required to protect the data controller's or data processor's legitimate interests, or legal needs, including possible litigation; or

(3) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

(e) *Duty to destroy personal data.* If a data controller or data processor obtains or stores personal data in violation of these Data Privacy Principles, it shall destroy the personal data unless an exception in subsection (d) above applies.

(f) *Policies and procedures.* A data controller and data processor shall develop written policies and procedures for the storage and destruction of personal data when developing policies and procedures is reasonable given the entity's size and the amount and sensitivity of the personal data that it stores. These procedures shall permit it to meet its obligations under this Section. A data controller or data processor shall also implement reasonable means for data destruction as part of its system design. These steps for data destruction shall take into account the cost of implementation and nature of risks to a data subject.

§ 11. Data Security and Data Breach Notification

(a) Reasonable security safeguards

(1) A data controller shall adopt reasonable security safeguards to protect against foreseeable risks, including unauthorized access, acquisition, use, modification, sharing, or destruction of personal data.

(2) Reasonable security safeguards are proportionate to the risk of harm in the event that the personal data is compromised. Proportionality is to be assessed in light of the type and nature of personal data used, the likely severity of harm to data subjects, the number of data subjects affected, and the cost of security safeguards.

(3) Reasonable security safeguards include administrative, physical, and technical measures that include training of employees.

(b) Personal-data-breach notification

(1) A personal-data breach is the unauthorized access, acquisition, use, modification, disclosure, or loss of personal data that compromises the privacy or security of the personal data.

(2) When a personal-data breach creates more than a low probability that personal data will be compromised, the data controller must notify affected data subjects without unreasonable delay, and must notify public authorities to the extent required by law.

(3) A data controller must provide a public notice for a personal-data breach that involves more than 500 data subjects.

(4) A data processor that has a personal-data breach shall notify the data controller as soon as reasonably possible. The data controller shall provide notice of a personal-data breach of its data processor as set forth in paragraphs (1), (2), and (3) above.

(5) The factors to be considered in determining whether there is a low probability that personal data will be compromised include:

(A) the nature and extent of the personal data involved, including the types of identifiers and the likelihood of re-identification;

(B) the identity of the unauthorized person to whom the personal data was disclosed or who used it;

(C) whether the personal data was actually acquired or accessed; and

(D) the extent to which the risk of compromise of the personal data has been mitigated.

(6) Notification is not required when the personal data was properly encrypted, and encryption keys are not compromised or breached.

§ 12. Onward Transfer

(a) *Limits on onward transfers.* A data controller or data processor that has personal data may make an onward transfers of this information to a data processor for personal-data activities only if:

(1) the data subject has received notice of the activities;

(2) the transfer is required by law; or

(3) the transfer is for uses specified in Principle 7(b) (exceptions to use limitation) and the requirements of Principle 7(b) and (c) are met.

(b) *Due diligence review of recipients of personal data.* Before making an onward transfer, a data controller or data processor shall exercise due diligence to ensure that the recipient will protect the personal data under these Principles.

(c) *Contracts with data processors.* Before making an onward transfer to a data processor, a data controller or data processor must enter into a binding contract with the recipient of the personal data. The contract shall include remedies for failing to comply with its terms, such as termination of the contract, and require the personal-data recipient to:

(1) protect the personal data according to these Principles;

(2) protect the personal data according to the transparency statement and individual notice;

(3) carry out only the personal-data activities that are necessary to comply with the contract or that are expressly authorized by the data controller or data processor that transferred the data; and

(4) take the following steps when transferring data to another data recipient:

(A) exercise due diligence;

(B) transfer data only to a recipient that will provide the required protection under (c)(1);

(C) enter into a contract that includes the same or greater protections as in its contract with the data controller and that requires the other data recipient to comply with the obligations of a data processor under this subsection;

(D) require that any subsequent data recipients do the same if they transfer the personal data to other downstream data recipients;

(5) notify the data controller of any onward transfer before it is made and allow the data controller to approve or reject the transfer;

(6) return or destroy the data at the data controller's request when the recipient no longer has a legal or contractual need to retain it;

(7) train its employees who have access to the personal data about their obligations under the Principles and their requirements under the transparency statements and individual notice from the data controller or data processor;

(8) devote appropriate resources, including sufficient personnel, to the protection of the personal data;

(9) facilitate the data controller's compliance with the Principles by cooperating with the data controller's oversight activities. The means of cooperation shall include providing information to the recipient that is required for compliance, and assisting the data controller when responding to a data subject's exercise of rights under these Principles. When necessary for the data controller's compliance with these Principles, cooperation shall extend even after the contract ends or is terminated.;

(10) develop and maintain a reasonable comprehensive privacy program as specified in Principle 13(c);

(11) make available information necessary for the data controller or data processor to evaluate the recipient's compliance with these Principles;

(12) notify the data controller promptly upon discovery of a personal-data breach or any noncompliance with the contract or this Principle, and cooperate fully with the data controller's efforts to address the matter; and

(d) *Reasonable oversight.* A data controller or data processor that transfers personal data shall engage in reasonable oversight of the recipient. If it finds that the recipient of the personal data is deficient in performing any of its contractual obligations related to this Principle, the data controller or data processor shall invoke appropriate measures under the contract to promptly resolve the deficiency, and also shall demand reasonable assurances from the personal-data recipient that the deficiency will not recur in the future.

(e) *Downstream onward transfers.* A data recipient that transfers personal data to a downstream data recipient shall follow the requirements of this Principle. Unless prohibited by law, every recipient of personal data, is covered by these Principles.

Chapter 3: Accountability and Enforcement

§ 13. Accountability

(a) Data controllers and data processors are accountable for complying with these Principles. Accountability by regularly assessing privacy and security risks associated with their data activities and maintaining a reasonable comprehensive privacy program of oversight and governance mechanisms.

(b) *Reasonable comprehensive privacy program.* A comprehensive privacy program is reasonable when it is appropriate to the entity's size, complexity, and resources; the amount and type of personal data used; and the risks that the entity's activities pose to the data subjects' privacy and security.

(c) *Components of a reasonable comprehensive privacy program.* A reasonable comprehensive privacy program shall include at least these components:

(1) written privacy and security policies and procedures with respect to all personal-data activities.

(2) a regular inventory of personal data collected, received, stored, or used that includes examination of:

(A) the types of data;

(B) the location of this personal data;

(C) the need to retain it;

(D) the protections that secure it;

(E) the individuals who have access to it; and

(F) the individuals responsible for overseeing its proper use and protection.

(3) a risk assignment conducted before a system goes live and at reasonable periodic intervals afterwards to identify and to fix, improve, and remedy within a reasonable period of time:

(A) any noncompliance or nontrivial risks of noncompliance with:

(i) these Data Privacy Principles;

(ii) applicable privacy or data-security laws;

(iii) its policies and procedures;

(B) the effectiveness of its policies and procedures and practices in light of the evolution of risks and the law; and

(C) the efficacy of its training of its workforce.

(4) a training program that reaches all employees or contractors who have access to or handle personal data, and employees or contractors whose actions materially affect the data that can be accessed or handled by others. This training shall be reasonably designed to permit the employee or contractor to understand the entity's policies and procedures and to be aware of and minimize any reasonably anticipated risks to personal data. At a minimum, training shall be conducted upon hiring or contracting and on an annual basis.

(d) Privacy and security by design

(1) A data controller or data processor shall analyze the privacy and security implications early on in the development of any new product, service, or process. This analysis shall be conducted in a reasonable manner, at a reasonable time, and with a reasonable thoroughness. This analysis shall be documented.

(2) A data controller or data processor shall examine how the product, service, or process should be designed to address the privacy or security issues identified in the analysis. The outcome of this examination shall be reflected in the final design of the product, service, or process. Reasonable design choices shall be made. Design choices and the reasoning that supports them shall be documented.

(e) Privacy and security by default

(1) A data controller or data processor shall analyze the default settings of any existing or new product or service and how such settings implicate privacy and security. This analysis shall be conducted in a reasonable manner, at a reasonable time, and with a reasonable thoroughness. This analysis shall be documented and repeated at reasonable intervals.

(2) A data controller or data processor shall draw on the outcome of this examination in the final default-setting choices that are made. Reasonable default-setting choices shall be made. Default-setting choices and the reasoning that supports them shall be documented.

§ 14. Enforcement

(a) To the extent that the law recognizes any remedies for these Principles, these remedies shall be effective, proportionate, and dissuasive.

(b) *Enforcement mechanisms.* Enforcement, if any, of these Principles can be through various mechanisms, including through individual redress and collective means of enforcement. Enforcement proceedings to enforce these Principles can include actions by the Federal Trade Commission, other governmental agencies, and state Attorneys General, as well as class-action

lawsuits and other civil proceedings involving the pursuit of civil remedies. Remedies can include compensation to injured parties, fines paid to the government, injunctions or administrative directives ordering future compliance, orders to comply, restitution of unjust enrichment, and other measures. Governmental decisionmakers may consider factors and elements that are not available to private parties claiming infringement.

(c) *Factors for deciding whether to provide remedies.* Factors to be considered in deciding on the remedies, if any, for the violation of a Principle include:

(1) the duty owed by one party to another, if any;

(2) the gravity of the infringement; any past infringements; mitigation and preventive actions taken by the data controller or data processor, including adherence to approved codes of conduct or safe harbors;

(3) the intentional or negligent character of the infringement;

(4) the unjust enrichment of a party by the use of personal data;

(5) the need for general deterrence of violations to effectuate a Principle.

(d) *Assessing the extent of the infringement.* The extent of the infringement may be determined by assessing the magnitude and likelihood of financial, reputational, or emotional harm, including the risk of such harm and the chilling effect on a data subject. The magnitude and likelihood of harm fall along a sliding scale. A significant risk may exist with a low likelihood of a high-magnitude injury or with a high likelihood of a low-magnitude injury. For a major potential injury, even a small likelihood may be a risk worthy of concern.

(e) *Future injury.* The magnitude and likelihood of future injury can be assessed by examining different factors. These include the types of personal data involved in a violation of a Principle, the means and methods used to exploit these types of data, their ability to be combined with other available data, and the types of harm and injury reasonably expected to result. A source of information to be drawn upon in evaluating these factors is the known injury, if any, to similarly situated victims.

(f) *The role of statutory law*. Statutory law can express these general principles by raising or lowering the thresholds for finding harm and specifying the kinds of harms that are remediable in different contexts.

(1) In some instances, a statute may deem certain legal violations of privacy interests as harmful per se with a designated minimum amount of statutory damages.

(2) Under some circumstances, the risk of future harm from a data-privacy violation may cause anxiety or emotional distress. Such harms may be compensable pursuant to statute or if recognized by courts.

(3) In some instances, a statute may use the unjust enrichment of a data controller through violation of these principles as a factor in assessing the extent of the infringement.